CS 3710: Introduction to Cybersecurity Final Exam, summer 2025

Name _____

Be sure to write your name and e-mail ID on top of this page.

If you are still writing when "pens down" is called, your exam will be ripped up and not graded. So please do that first. Sorry to have to be strict on this!

There are 6 pages to this exam. Once the exam starts, please make sure you have all the pages. Questions are worth different amounts of points.

Answers for the short-answer questions should not exceed about 20 words; if your answer is too long (say, more than 30 words), you will get a zero for that question!

This exam is CLOSED text book, closed-notes, closed-calculator, closed-cell phone, closed-computer, closed-neighbor, etc. Questions are worth different amounts, so be sure to look over all the questions and plan your time accordingly. Please sign the honor pledge below.

_____

_____

_____

_____

Free public WiFi

Is it really safe to use?

Ask Man in Middle

Page 2: Midterm material

1. [3 points] Briefly explain how RSA can sign a message.

2. [3 points] *Briefly,* what prevents a MITM (in-the-middle) attack against the TLS protocol?

3. [6 points] Name and *briefly* describe each of the four ethical frameworks discussed in class.

Page 3: Binary Exploits

4. [6 points] Write a simple x86 encryptor for a virus. Minor assembly compilation errors are not a problem – as long as it's clear assembly to thsoe grading it. If you can't write the assembly, write pseudo-code, which will get you partial credit. We are not looking for any advanced encryption here. If your code is more than 10 assembly opcodes, it won't be graded.

5. [3 points] Briefly, how does a buffer overflow attack work? This needs to be 30 words or less!

6. [3 points] What is the difference between oligomorphic, polymorphic, and metamorphic viruses? If you get the definitions right, but mix up which word each definition is for, you will still get a majority of the credit.

Page 4: SQL, XSS, CSRF, and Stuxnet

7. [3 points] Briefly, give two ways to prevent against SQL injection attacks.

8. [3 points] Briefly, give a real-world example of an cross-site scripting attack.

9. [3 points] Briefly, why do we care about CSRF?

10. [3 points] Briefly, what were the two most impressive aspects of Stuxnet?

Page 5: Anonymity and Cryptocurrency

11. [3 points] Imagine that you are a "rebel" in a given country, and the government is watching you. They are analyzing all of your communication, and – given any amount of evidence – they would arrest you. Assume that you can install any software that exists – it's only networking communications that are monitored. Briefly, how would you communicate with another "rebel" without getting caught? State any *reasonable* assumptions that you make.

12. [3 points] Briefly, how does one contact a hidden service in Tor?

13. [3 points] Briefly, what is blockchain? Briefly, how does it work?

14. [3 points] Briefly, what is the *difficulty* metric of Bitcoin?

Page 6: Forensics, Rootkits, and VMs

15. [3 points] Briefly, what was the FBI-Apple encryption dispute about?

16. [3 points] Briefly, when is the government allowed to extract the password from you for your encrypted hard drive?

17. [3 points] Briefly, give one advantage and one disadvantage for each of the two types of rootkits.

18. [3 points] Briefly describe each of the four levels of virtual machines.